UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

RAYMOND J. BARKLEY, individually and on behalf of all others similarly situated, Plaintiff, v. MARRIOTT INTERNATIONAL, INC., Defendant.	Case No. COMPLAINT AND DEMAND FOR JURY TRIAL

NATURE OF THE ACTION

1. Plaintiff brings this class action against Marriott International, Inc. ("Marriott"), parent of Starwood Hotels & Resorts Worldwide, LLC ("Starwood"), for its failure to secure and safeguard hundreds of millions of Starwood's customers' personally identifiable information ("PII"), including highly sensitive information such as passport information, credit and debit card numbers, and other payment card data. Starwood collected this information at the time customers registered on its website, checked in at any of its properties, or used its loyalty program.

2. In 2014 (or even earlier), hackers broke into Starwood's information systems to steal confidential and sensitive guest data for hundreds of millions of customers (the "Data Breach"). The hackers' efforts continued through early September 2018, allowing the hackers access to PII for Starwood guests for at least four years.

3. Incredibly, despite the Data Breach first occurring at least four years ago, neither Starwood nor Marriott discovered the breach until September 2018. Even then, Marriott—responsible for Starwood's systems since the completion of its acquisition—failed to notify customers about the breach until nearly three months later on November 30, 2018.

4. Finally, after years of not even so much as detecting the Data Breach, and then months of hiding the Data Breach from the public, Marriott issued a press release conceding that an investigation had determined that there was unauthorized access to the Starwood guest reservation database, which contained guest information relating to reservations at Starwood properties on or before September 10, 2018.

5. Marriott has not completed its identification of duplicate information in the database, but the company believes it contains information on up to approximately 500 million guests who made a reservation at a Starwood property. For approximately 327 million of these guests, the information includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. For some, the information also includes payment card numbers and payment card expiration dates.

6. Marriott could have prevented this Data Breach with tighter security protocols. Many hotel operators fail to use the same level of security systems required by financial institutions and other highly regulated industries, but hospitality companies—like Marriott and Starwood—house incredibly sensitive information.

7. Indeed, the most secure information systems (which are entirely appropriate since Marriott was hosting sensitive passport and payment information on its systems) ensure that data is safely secured and also ensure that, in the event encrypted data is inadvertently leaked, hackers cannot access the encryption keys that decrypt that same data. Marriott failed on both accounts.

8. Marriott disregarded Plaintiff's and Class Members' rights by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its

data systems were protected, failing to take available steps to prevent and stop the breach from ever happening, and failing to disclose to its customers the material facts that it did not have adequate computer systems and security practices to safeguard customers' confidential and sensitive information.

9. On information and belief, the data at issue here was not kept in accordance with applicable, required, and appropriate cyber-security protocols, policies, and procedures. As a result, Plaintiff's and Class Members' information was compromised and stolen.

10. Relatedly, because the data remains stored on Marriott's information systems, Plaintiff and Class Members have an interest in ensuring that their information is safe, and they are entitled to seek injunctive and other equitable relief.

PARTIES

11. Plaintiff, Raymond J. Barkley, is a resident of the state of New York. Mr. Barkley is and was a Starwood Platinum Preferred Guest Member during the relevant time period. Plaintiff repeatedly provided his personal and confidential information to Defendant in connection with reservations, including stays at W Hotels in Barcelona, Spain, Fort Lauderdale, Florida, and Atlanta, Georgia, Westin Hotels in New York, New York, and Princeton, New Jersey, and Sheraton Hotels in Boston, Massachusetts, and Baltimore, Maryland, on the basis that Defendant would keep his information secure, and employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and notify him promptly in the event of a breach. Marriott and Starwood notified Plaintiff via email on December 9, 2018, that his information was compromised during the data breach. As a result of the breach, Mr. Barkley has spent numerous hours monitoring his accounts to ensure that his identity is not stolen and that his accounts are not compromised.

12. Marriott International, Inc. is a Delaware corporation with its principal place of business in Bethesda, MD. Marriott primarily derives its revenues from hotel and restaurant operations, and it operates more than 6,700 properties across 130 countries and territories. Its brands include Marriott, Starwood, and The Ritz-Carlton. Starwood, which operates popular properties such as Westin, Sheraton, and St. Regis, is a wholly-owned subsidiary of Defendant Marriott.

JURISDICTION AND VENUE

13. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). The aggregated claims of the individual class members exceed $5,000,000.00, exclusive of interest and costs, and this is a class action in which more than two-thirds of the proposed plaintiff class, on the one hand, and Marriott, on the other, are citizens of different states.

14. This Court has jurisdiction over Marriott because it is authorized to conduct business throughout the United States, including New York; it owns and operates many hotels throughout New York and the United States; and it advertises in a variety of media throughout the United States, including New York. Via its business operations throughout the United States, Marriott intentionally avails itself of the markets within this state to render the exercise of jurisdiction by this Court just and proper.

15. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District and because Plaintiff is a resident of New York.

FACTUAL BACKGROUND

A. Marriott Gathers Massive Amounts of Private Information from Its Guests.

16. The Marriott hotel chain operates more than 6,700 properties around the world.

17. In November 2015, Marriott announced that it was purchasing Starwood for $13.6 billion, creating the world's largest hotel empire. Marriott later completed that acquisition by September 2016, expanding its global presence.

18. Starwood includes the following hotel brands: W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Meridien Hotels & Resorts, Four Points by Sheraton, and Design Hotels, as well as Starwood-branded timeshare properties.

19. Despite the acquisition of Starwood, Marriott apparently still maintains separate guest reservation and/or information systems for Marriott-branded properties versus Starwood-branded properties.

20. Marriott maintains a Global Privacy Statement on its website, informing guests about the company's privacy policies. That Privacy Statement states:

> This Privacy Statement describes the privacy practices of the Marriott Group for data that we collect:
>
> - through websites operated by us from which you are accessing this Privacy Statement, including Marriott.com and other websites owned or controlled by the Marriott Group (collectively, the "**Websites**")
> - through the software applications made available by us for use on or through computers and mobile devices (the "**Apps**")
> - through our social media pages that we control from which you are accessing this Privacy Statement (collectively, our "**Social Media Pages**")
> - through HTML-formatted email messages that we send you that link to this Privacy Statement and through your communications with us
> - when you visit or stay as a guest at one of our properties, or through other offline interactions
>
> Collectively, we refer to the Websites, the Apps and our Social Media Pages, as the "**Online Services**" and, together with offline channels, the "**Services**." By

using the Services, you agree to the terms and conditions of this Privacy Statement.

"**Personal Data**" are data that identify you as an individual or relate to an identifiable individual.

At touchpoints throughout your guest journey, we collect Personal Data in accordance with law, such as:

- Name
- Gender
- Postal address
- Telephone number
- Email address
- Credit and debit card number or other payment data
- Financial information in limited circumstances
- Language preference
- Date and place of birth
- Nationality, passport, visa or other government-issued identification data
- Important dates, such as birthdays, anniversaries and special occasions
- Membership or loyalty program data (including co-branded payment cards, travel partner program affiliations)
- Employer details
- Travel itinerary, tour group or activity data
- Prior guest stays or interactions, goods and services purchased, special service and amenity requests
- Geolocation information
- Social media account ID, profile photo and other data publicly available, or data made available by linking your social media and loyalty accounts

In more limited circumstances, we also may collect:

- Data about family members and companions, such as names and ages of children
- Biometric data, such as digital images
- Images and video and audio data via: (a) security cameras located in public areas, such as hallways and lobbies, in our properties; and (b) body-worn cameras carried by our loss prevention officers and other security personnel
- Guest preferences and personalized data ("**Personal Preferences**"), such as your interests, activities, hobbies, food and beverage choices, services and amenities of which you advise us or which we learn about during your visit

> If you submit any Personal Data about other people to us or our Service Providers (e.g., if you make a reservation for another individual), you represent that you have the authority to do so and you permit us to use the data in accordance with this Privacy Statement.[1]

21. Marriott states that it collects personal data through, among other sources, online services, property visits, customer care centers, strategic business partners, and internet-connected devices at their properties.

22. Marriott stores massive amounts of personal information on its servers and utilizes this information to maximize its profits through predictive marketing and other marketing techniques.

23. Consumers place tremendous value in data privacy and security, and they consider it when making decisions on where to stay for travel. Plaintiff would not have stayed at the Starwood hotels nor would he have used his debit or credit cards to pay for his Starwood stays had he known that Marriott does not take all necessary precautions to secure consumers' personal and financial data.

24. Marriott failed to disclose its negligent and insufficient data security practices, and consumers relied on or were misled by its omission.

B. Marriott Took Four Years to Discover the Data Breach and Even Then Delayed Informing Impacted Customers.

25. On September 8, 2018, Marriott received an alert from an internal system that there was an attempt to access the Starwood guest reservation database.

26. Marriott began to investigate the attempt and learned that unauthorized users had gained access to the Starwood network since 2014 – *four years* before detection.

[1] https://www.marriott.com/about/privacy.mi (last accessed Dec. 5, 2018).

27. The investigation further revealed that the unauthorized users had copied and encrypted information, as well as attempted to remove (or "exfiltrate") it.

28. On November 19, 2018, Marriott decrypted the information and confirmed that the contents were from its Starwood guest reservation database.

29. Marriott has confirmed that, subject to de-duplicating its records, approximately 500 million guests who made a reservation at a Starwood property since 2014 may have been impacted.

30. The database contains approximately 327 million guests' information including some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences.

31. For other guests, the information also includes payment card numbers and payment card expiration dates.

32. Other guests' accounts included a name and potentially a mailing address, email address, or other information.

33. According to Gus Hosein, executive director of Privacy International, "They can say all they want that they take security seriously, but they don't if you can be hacked over a four-year period without noticing."[2]

[2] *See* Nicole Perlroth, Amie Tsang and Adam Satariano, *Marriott Hacking Exposes Data of Up to 500 Million Guests*, N.Y. Times (Nov. 30, 2018), https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html (last accessed Dec. 5, 2018).

34. Recent news reports indicate that hackers working on behalf of China's primary intelligence agency may have been responsible for the breach,[3] but regardless of the ultimate identity of the hackers, Marriott failed its customers on many levels.

C. Stolen Private Information is Valuable to Hackers and Thieves.

35. It is well known and the subject of many media reports that PII data is highly coveted and a frequent target of hackers. PII data is often easily taken because it may be less protected and regulated than payment card data.

36. In the hospitality industry, many companies have been the targets of data breaches. Moreover, Marriott (and Starwood) was aware or should have been aware of the federal government's heightened interest in securing consumers' PII when staying in hotels located in the United States due to the very public litigation commenced by the Federal Trade Commission against Wyndham Worldwide Corporation founded upon that company's failure to provide reasonable cybersecurity protections for customer data.

37. Despite this well-publicized litigation and the frequent public announcements of data breaches by retailers and hotel chains, Marriott opted to maintain an insufficient and inadequate system to protect the PII of Plaintiff and Class Members.

38. Hotels are often attractive targets for hackers because they do not maintain the same security standards as financial institutions, despite housing much of the same sensitive data and information.

39. Biographical data is also highly sought after by data thieves. PII data has been stolen and sold by the criminal underground on many occasions in the past, and the accounts of

---

[3] Michael Balsamo, *China Suspected in Huge Marriott Data Breach, Official Says*, AP (Dec. 12, 2018), https://www.apnews.com/4032b90c40824fbb892206702c5d30ad (last accessed on Dec. 19, 2018).

theft and unauthorized access have been the subject of many media reports. One form of identity theft, branded "synthetic identity theft," occurs when thieves create new identities by combining real and fake identifying information and then using those identities to open new accounts.

40. Despite all of this, Marriott's security protocols were wholly inadequate to protect against this magnitude of a data breach. At the very minimum, Marriott acted negligently, if not recklessly.

D. This Data Breach Will Result In Additional Identity Theft and Identify Fraud.

41. Marriott failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach.

42. The ramifications of Marriott's failure to keep Plaintiff's and Class Members' data secure are severe.

43. The information Marriott compromised, including Plaintiff's identifying information and/or other financial information, is incredibly valuable to identity thieves. Identity theft occurs when someone uses another's personal identifying information, such as that person's name, address, credit card number, credit card expiration date, and other information, without permission, to commit fraud or other crimes.

44. The FTC estimates that as many as ten million Americans have their identities stolen each year. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account [as occurred to Plaintiff here], run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[4]

[4] Fed. Trade Comm'n, Signs of Identity Theft, http://www.consumer.ftc.gov/articles/ 0271-signs-identity-theft (last visited Nov. 30, 2018).

45. According to Javelin Strategy and Research, "1 in 4 data breach notification recipients became a victim of identity fraud."[5] Nearly half (46%) of consumers with a breached debit card became fraud victims within the same year.

46. Identity thieves can use personal information such as that of Plaintiff and Class Members, which Marriott failed to keep secure, to perpetrate a variety of crimes that harm victims.

47. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund. Some of this activity may not come to light for years.

48. Among other forms of fraud, identity thieves may obtain medical services using consumers' compromised personal information or commit any number of other frauds, such as obtaining a job, procuring housing, or providing false information to police during an arrest.

49. Even with financial reimbursement, the harm will continue for any affected individuals. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."[6] In fact, victims may need more than one year to resolve identity theft problems.[7]

---

[5] *See* Al Pascual, *2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters*, Javelin (Feb. 20, 2013), *available at* www.javelinstrategy.com/brochure/276 (last visited Nov. 30, 2018) (the "2013 Identity Fraud Report").

[6] Victims of Identity Theft, 2012 (Dec. 2013), at 10, http://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited Sept. 24, 2018).

[7] *Id.* at 11.

E. Annual monetary Losses from Identity Theft are in the Billions of Dollars.

50. Over the past five years, the cost of identity theft losses can reach anywhere from $17 billion to nearly $22 billion in any given year.

51. Additionally, there may be a gap between when harm occurs versus when it is discovered, and between when information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"):

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[8]

52. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, whether such charges are ultimately reimbursed by the credit card companies.

F. Marriott Is Already Experiencing Problems With Its Response to the Data Breach.

53. While Marriott set up a dedicated website and call center to handle inquiries following its announcement of the Data Breach, the incredible number of impacted guests has meant long wait times, and the lack of information about who was impacted and how has left millions of customers confused and worried.

---

[8] *Report to Congressional Requesters: Personal Information, Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), at 33, http://www.gao.gov/new.items/d07737.pdf (emphases added) (last visited Sept. 24, 2018).

54. Further, the one year of free enrollment in Web Watcher (offered as an apparent token of good will) only applies to guests who live in the United States, Canada, and Britain, and it is not a credit monitoring service. Web Watcher merely monitors certain activity on the "Deep Web" (a portion of the internet where hackers often sell personal information and data).

55. The Web Watchers program may detect some illegal activity, but it cannot alone identify and prevent identity theft.

56. Moreover, credit monitoring is another critical tool to consumers concerning about identity theft—a tool not currently offered by Marriott to affected individuals.

G. Plaintiff and Class Members Suffered Damages.

57. The Data Breach was a direct and proximate result of Marriott's failure to properly safeguard and protect Plaintiff's and Class Members' private information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Marriott's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

58. Plaintiff's and Class members' PII is private and sensitive in nature and was left inadequately protected by Marriott. Marriott did not obtain Plaintiff's and Class Members' consent to disclose their PII to any other person as required by applicable law and industry standards.

59. As a direct and proximate result of Marriott's wrongful action and inaction and the resulting Data Breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take significant time and effort to mitigate the actual and potential impact of the Data

Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

60. Marriott's deep regrets are no comfort to Plaintiff and Class Members, though undoubtedly they agree that Marriott fell short of what its guests deserve.

61. Marriott's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' Private Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

(a) theft of their personal and financial information;

(b) the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their passport, credit/debit card, and personal information being placed in the hands of criminals;

(c) the untimely and inadequate notification of the Data Breach;

(d) the improper disclosure of their information;

(e) loss of privacy;

(f) ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

(g) ascertainable losses in the form of deprivation of the value of their information, for which there is a well-established national and international market;

(h) overpayments to Marriott for products and services purchased during the Data Breach in that a portion of the price paid for such products and services by Plaintiff and Class Members to Marriott was for the costs of reasonable and adequate safeguards and security

measures that would protect customers' information and data, which Marriott did not implement and, as a result, Plaintiff and Class members did not receive what they paid for and were overcharged by Marriott;

(i) the loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts; and

(j) deprivation of rights they possess under various state laws.

62. While the information of Plaintiff and Class Members has been stolen, the same or a copy of such data continues to be held by Marriott. Plaintiff and Class Members have an undeniable interest in insuring that this information is secure, remains secure, and is not subject to further theft.

FRAUDULENT CONCEALMENT AND TOLLING OF STATUTE OF LIMITATIONS

63. Plaintiff's claims arise out of the Marriott's fraudulent concealment of the Data Breach. To the extent that Plaintiff's claims arise from Marriott's fraudulent concealment, there is no one document or communication, and no one interaction, upon which Plaintiff bases his claims. Marriott was under a duty to disclose the Data Breach based upon their exclusive knowledge of such occurrence, but Marriott never disclosed the Data Breach to Plaintiff or the public at any time or place or in any manner until November 30, 2018—four years after the initial hack and months after Marriott's discovery of such hack.

64. The tolling doctrine was made for cases of concealment like this one. For the following reasons, any otherwise-applicable statutes of limitations have been tolled by the discovery rule with respect to all claims.

65. Through the exercise of reasonable diligence, and within any applicable statutes of limitations, Plaintiff and members of the proposed Class could not have discovered that Marriott suffered such a massive data breach.

66. Plaintiff and the other Class members could not reasonably discover, and did not know of facts that would have caused a reasonable person to suspect, that Marriott suffered such a significant data breach, nor could Plaintiff or Class Members know that Marriott was four years late in recognizing such a breach.

67. Throughout the relevant time period, all applicable statutes of limitations have been tolled by Marriott's knowing and active fraudulent concealment and denial of the facts alleged in this Complaint.

68. Instead of disclosing its Data Breach, Marriott kept the incident confidential and failed to alert its customers that their personal information had been breached for up to four years (or more).

69. Thus, Marriott is estopped from relying on any statutes of limitations in defense of this action.

CLASS ACTION ALLEGATIONS

70. Plaintiff seeks relief in his individual capacity and as a representative of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a) and (b)(2), (b)(3), and (c)(4), Plaintiff seeks certification of a Nationwide class as described herein. The national class is initially defined as follows: all persons in the United States whose personal and/or financial information was disclosed in the Data Breach affecting Marriott from 2014 to 2018 (the "Nationwide Class").

71. Excluded from the Class are Marriott, including any entity in which Marriott has a controlling interest, is a parent or subsidiary, or which is controlled by Marriott, as well as the

officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Marriott. Also excluded are the judges and court personnel in this case and any members of their immediate families.

72. **Numerosity:** Fed. R. Civ. P. 23(a)(1). The members of the Classes are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. While Plaintiff is informed and believes that there are not less than hundreds of millions of members of the Classe the precise number of Class members is unknown to Plaintiff, but may be ascertained from Marriott's records. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, Internet postings, and/or published notice.

73. **Commonality and Predominance:** Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

(a) Whether Marriott violated the various state consumer protection laws by failing to implement reasonable security procedures and practices;

(b) Whether Marriott violated state or federal laws by failing to detect the Data Breach at an earlier date;

(c) Whether Marriott violated state or federal laws by failing to promptly notify class members that their personal information had been compromised;

(d) Whether class members may obtain injunctive relief against Marriott under privacy laws to require that it safeguard or destroy, rather than retain, personal information;

(e) Which security procedures and which data breach notification procedure should Marriott be required to implement as part of any injunctive relief ordered by the Court;

(f) Whether Marriott has an implied contractual obligation to use reasonable security measures;

(g) Whether Marriott has complied with any implied contractual obligation to use reasonable security measures;

(h) What security measures, if any, must be implemented by Marriott to comply with its implied contractual obligations;

(i) Whether Marriott violated state privacy laws in connection with the actions described herein; and

(j) What the nature of the relief should be, including equitable relief, to which Plaintiff and the Class members are entitled.

74. All members of the proposed Class are readily ascertainable. Marriott has access to addresses and other contact information for millions of members of the Class, which can be used for providing notice to many Class members.

75. **Typicality:** Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class members because Plaintiff's information, like that of every other Class Member, was part of the Data Breach resulting from Marriott's failure to safeguard such information.

76. **Adequacy of Representation:** Fed. R. Civ. P. 23(a)(4). Plaintiff is an adequate Class representative because his interests do not conflict with the interests of the other members of the Class he seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation; and Plaintiff intends to prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and his counsel.

77. **Superiority of Class Action:** Fed. R. Civ. P. 23(b)(3). A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Marriott, so it would be impracticable for members of the Class to individually seek redress for the wrongful conduct.

78. **Declaratory and Injunctive Relief:** Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Marriott has acted or refused to act on grounds generally applicable to Plaintiff and the other members of the Class, thereby making appropriate final injunctive relief and declaratory relief, as described below, with respect to the Class as a whole.

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Nationwide Class)

79. Plaintiff incorporates by reference all preceding allegations as though fully set forth herein.

80. Defendant solicited and invited Plaintiff and Class Members to join its Loyalty Program, which required that Plaintiff and Class members share personal information such as dates of birth, passport numbers, credit and debit card numbers and other payment data, employer details, geolocation information, and other personal and confidential information as described herein.

81. Defendant then invited Plaintiff and Class Members to continually use its Loyalty Program to book rooms, and earn and redeem rewards. Plaintiff and Class Members accepted

certain offers made by Defendant in connection with use of the Loyalty Program, continuing to allow Defendant to store, maintain, and safeguard their personal and confidential information.

82. When Plaintiff and Class Members provided their personal and confidential information to Defendant in connection with joining the Loyalty Program, they entered into implied contracts with the Defendant, pursuant to which Defendant agreed to safeguard and protect their information, and to timely and accurately notify Plaintiff and Class Members if their data had been breached or compromised.

83. Plaintiff and Class Members would not have provided and entrusted their personal and confidential information to Defendant in connection with joining Defendant's loyalty program in the absence of the implied contract between them.

84. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

85. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect the personal and confidential information of Plaintiff and Class Members and by failing to provide timely and accurate notice to them that their information was compromised in and as a result of the Data Breach.

86. As a direct and proximate result of Defendant's breaches of the implied contracts between Defendant and Plaintiff and Class Members, Plaintiff and Class Members sustained actual losses and damages as described in detail herein.

SECOND CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

87. Plaintiff incorporates by reference all preceding allegations as though fully set forth herein.

88. Upon accepting and storing Plaintiff's and Class Members' personal and confidential information in its respective computer database systems, Defendant undertook and owed a duty to Plaintiff and Class Members to exercise reasonable care to secure and safeguard that information and to utilize commercially reasonable methods to do so. Defendant knew, acknowledged, and agreed the information was private and confidential and would be protected as private and confidential.

89. The law imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of personal and confidential information to Plaintiff and the Class, so Plaintiff and Class Members could take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their information.

90. Defendant breached its duty to notify Plaintiff and Class Members of the unauthorized access by failing to notify Plaintiff and Class Members of the Data Breach until November 30, 2018. To date, although it has been months since the breach was discovered, and four years since the breach commenced, Defendant has not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and the Class.

91. Defendant also breached its duty to Plaintiff and the Class Members to adequately protect and safeguard this information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to Plaintiff's and Class Members' private information. Furthering its dilatory practices, Defendant failed to provide adequate oversight of the private information to which it was entrusted, resulting in a massive breach of the personal and confidential information of potentially 500 million people, undetected over a period of four years.

92. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect Plaintiff's and Class Members' personal and confidential information from being foreseeably captured, accessed, disseminated, stolen, and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class Members' information during the time it was within Defendant's possession or control.

93. Further, through Defendant's failure to provide timely and clear notification of the Data Breach to consumers, Defendant prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their financial data and bank accounts.

94. Upon information and belief, Defendant improperly and inadequately safeguarded the personal and confidential information of Plaintiff and Class Members in deviation from standard industry rules, regulations, and practices at the time of the Data Breach.

95. Defendant's failure to take proper security measures to protect Plaintiff's and Class Members' sensitive personal and confidential information violated its duty to protect that data and prevent its dissemination to third parties.

96. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices. By collecting and maintaining personal and confidential information of the Plaintiff and Class Members, and acknowledging that this information needed to be kept secure, it was foreseeable that they would be harmed in the future, if Defendant did not protect Plaintiff's and Class Members' information from hackers.

97. Defendant's duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting

commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal and confidential information. Various FTC publications and data security breach orders further form the basis of Defendant's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

98. Defendant's acknowledged the importance of keeping this information secure, and stated that they sought "to use reasonable organizational, technical and administrative measures to protect Personal Data."[9] Despite acknowledging their responsibility to keep this information secure, Defendant improperly put the burden on Plaintiff and Class Members to notify Defendant if they suspected that their information was not secure, when individuals would not have access to this information, and Defendant was in a superior position to know this information and was in the exclusive possession of such information.[10]

99. Upon information and belief, Defendant improperly and inadequately safeguarded the personal and confidential information of Plaintiff and Class Members in deviation from standard industry rules, regulations, and practices at the time of the Data Breach.

100. Defendant's failure to take proper security measures to protect Plaintiff's and Class Members' sensitive personal and confidential information has caused Plaintiff and Class Members to suffer injury and damages. As described herein, Plaintiff received notice that his information was compromised, and now must take and has taken affirmative steps to ensure that his identity is not stolen and his financial information is not compromised.

---

[9] *See* Marriott, Marriott Group Global Privacy Statement, https://www.marriott.com/about/privacy.mi (follow "Security" link) (last accessed Dec. 21, 2018).

[10] *Id.*

THIRD CAUSE OF ACTION
MARYLAND PERSONAL INFORMATION PROTECTION ACT
Md. Code Com. Law §§ 14-3501, *et seq.*
(On Behalf of Plaintiff and the Nationwide Class)

101. Plaintiff incorporates by reference all preceding allegations as though fully set forth herein.

102. Included in the terms and conditions of the Loyalty Program is a Choice of Law and Venue Provision that provides that Maryland law applies to the Loyalty Program.

103. Under Md. Code Com. Law § 14-3503(a), "[t]o protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of personal information owned or licensed and the nature and size of the business and its operations."

104. Defendant is a business that owns or licenses computerized data that includes Personal Information as defined by Md. Code Com. Law§§ 14-3501(b)(1) and (2).

105. Plaintiff and Class Members are "individuals" and "customers" as defined and covered by Md. Code Com. Law §§ 14-3502(a) and 14-3503.

106. Plaintiff's and Class Members' private information, as described herein and throughout, includes Personal Information as covered under Md. Code Com. Law § 14-3501(e)(1).

107. Defendant did not maintain reasonable security procedures and practices appropriate to the nature of the Personal Information owned or licensed and the nature and size of its business and operations in violation of Md. Code Com. Law § 14-3503.

108. The Data Breach was a "[b]reach of the security of a system" as defined by Md. Code Com. Law § 14-3504(a)(1).

109. Under Md. Code Com. Law § 14-3504(b)(1), "[a] business that owns or licenses computerized data that includes personal information of an individual residing in the State, when it discovers or is notified of a breach of the security system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information of the individual has been or will be misused as a result of the breach."

110. Under Md. Code Com. Law §§ 14-3504(b)(2) and 14-3504(c)(2), "[i]f, after the investigation is concluded, the business determines that the breach of the security of the system creates a likelihood that personal information has been or will be misused, the business shall notify the individual of the breach" and that notification "shall be given as soon as reasonably practicable, but not later than 45 days after the business discovers or is notified of the breach of the security of a system."

111. Because Defendant discovered a security breach and had notice of a security breach, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Md. Code Com. Law §§ 14-3504(b)(2) and 14-3504(c)(2).

112. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated Md. Code Com. Law §§ 14-3504(b)(2) and 14-3504(c)(2).

113. As a direct and proximate result of Defendant's violations of Md. Code Com. Law §§ 14-3504(b)(2) and 14-3504(c)(2), Plaintiff and Class Members suffered damages, as described above.

114. Pursuant to Md. Code Com. Law e § 14-3508, Defendant's violations of Md. Code Com. Law §§ 14-3504(b)(2) and 14-3504(c)(2) are unfair or deceptive trade practices within the meaning of the Maryland Consumer Protection Act, 13 Md. Code Com. Law §§ 13-

101, *et seq.* and subject to the enforcement and penalty provisions contained within the Maryland Consumer Protection Act.

115. Plaintiff and Class Members seek relief under Md. Code Com. Law §13-408, including actual damages and attorney's fees.

FOURTH CAUSE OF ACTION
MARYLAND CONSUMER PROTECTION ACT,
Md. Code Com. Law §§ 13-301, *et seq.*
(On Behalf of Plaintiff and the Nationwide Class)

116. Plaintiff incorporates by reference all preceding allegations as though fully set forth herein.

117. Included in the terms and conditions of the Loyalty Program is a Choice of Law and Venue Provision that provides that Maryland law applies to the Loyalty Program.

118. To the extent Maryland law does not apply, Plaintiff brings this claim on behalf of himself and Class Members on behalf of applicable state consumer protection and deceptive business practices acts.

119. Defendant is a "person" as defined by Md. Code Com. Law§ 13-101(h).

120. Defendant's conduct as alleged herein related to "sales," "offers for sale," or "bailment" as defined by Md. Code Com. Law§ 13-101(i) and § 13-303.

121. Plaintiff and Class Members are "consumers" as defined by Md. Code Com. Law§ 13-101(c).

122. Defendant advertises, offers, or sells "consumer goods" or "consumer services" as defined by Md. Code Com. Law§ 13-101(d).

123. Defendant advertised, offered, or sold goods or services in Maryland and engaged in trade or commerce directly or indirectly affecting the people of Maryland.

124. Defendant engaged in unfair and deceptive trade practices, in violation of Md. Code Com. Law§ 13-301, including:

(a) False or misleading oral or written representations that have the capacity, tendency, or effect of deceiving or misleading consumers;

(b) Failing to state a material fact where the failure deceives or tends to deceive;

(c) Advertising or offering consumer goods or services without intent to sell, lease, or rent them as advertised or offered;

(d) Deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with the promotion or sale of consumer goods or services or the subsequent performance with respect to an agreement, sale lease or rental.

125. Defendant engaged in these unfair and deceptive trade practices in connection with offering for sale or selling consumer goods or services or with respect to the extension of consumer credit, in violation of Md. Code Com. Law§ 13-303, including:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class Members' personal and confidential information, which was a direct and proximate cause of the Data Breach;

(b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

(c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' personal and confidential information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and the Maryland Personal Information Protection Act, Md. Code Com. Law§ 14-3503, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' personal and confidential information, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and the Maryland Personal Information Protection Act, Md. Code Com. Law§ 14- 3503;

(f) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' information; and

(g) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and the Maryland Personal Information Protection Act, Md. Code Com. Law§ 14-3503.

126. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' personal and confidential information. Defendant's

misrepresentations and omissions would have been important to a significant number of consumers in making financial decisions.

127. Defendant intended to mislead Plaintiff and Class Members and induce them to rely on its misrepresentations and omissions.

128. Had Defendant disclosed to Plaintiff and Class Members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue its Loyalty Program and it would have been forced to adopt reasonable data security measures and comply with the law.

129. Defendant acted intentionally, knowingly, and maliciously to violate Maryland's Consumer Protection Act, and recklessly disregarded Plaintiff's and Class Members' rights. Defendant was on notice of the possibility of the Data Breach due to its prior data breach and infiltrations of its systems.

130. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

131. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

REQUEST FOR RELIEF

132. **WHEREFORE**, Plaintiff, individually and on behalf of all Class Members proposed in this Complaint, respectfully requests that the Court enter judgment in his favor and against Marriott as follows:

(a) Certification of the proposed Classes, including appointment of Plaintiff's counsel as Class Counsel;

(b) For an order temporarily and permanently enjoining Marriott from continuing the unlawful, deceptive, fraudulent, and unfair business practices alleged in this Complaint;

(c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity to Class members the type of information compromised;

(d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

(e) For an award of actual damages and compensatory damages, in an amount to be determined;

(f) For treble and/or punitive damages as permitted by applicable laws;

(g) For an award of costs of suit and attorneys' fees; and

(h) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff demands a jury trial on all issues so triable.

Dated: January 9, 2018

Respectfully submitted,

By: /s/ Michael P. Canty
Michael P. Canty
Brian R. Morrison (*pro hac vice* application to be submitted)
LABATON SUCHAROW LLP
140 Broadway
New York, NY 10005
Telephone: 212-907-0700
Facsimile: 212-818-0477
Email: mcanty@labaton.com
bmorrison@labaton.com

Counsel for the Plaintiff and the Proposed Class